ACTA ARITHMETICA
134.1 (2008)

Distribution of consecutive modular roots of an integer

by

JEAN BOURGAIN (Princeton, NJ) and IGOR E. SHPARLINSKI (Sydney)

1. Introduction. For a prime p we denote by $\mathbb{F}_p$ the finite field of p elements, which we assume to be represented by the set $\{0, 1, \ldots, p-1\}$. For an integer t we denote by $\mathbb{Z}_t$ the residue ring modulo t and by $\mathbb{Z}_t^*$ the group of units of $\mathbb{Z}_t$.

Let $\vartheta \in \mathbb{F}_p^*$ be of multiplicative order $t \ge 1$. There is a rather long history of studying the exponential sums with the powers ϑ^n, $n = M+1, \ldots, M+N$, where $N \le t$, in finite fields and residue rings: see [6, 7, 17, 21–23, 26–28] for several results in this direction together with their numerous applications.

Here we consider a presumably harder question about exponential sums with the roots $\vartheta^{1/n}$, for $n = M+1, \ldots, M+N$ with $\gcd(n,t) = 1$ instead of the powers. More precisely, for an integer $m > 0$, we put

$$\mathbf{e}_m(z) = \exp(2\pi i z/m),$$

and define the sums

$$S_a(M,N) = \sum_{\substack{n=M+1 \\ \gcd(n,t)=1}}^{M+N} \mathbf{e}_p(a\vartheta^{1/n}), \qquad a \in \mathbb{F}_p,$$

to which previously known techniques do not seem to apply.

We show that a different approach, which makes use of recent results of [5] on exponential sums with sparse polynomials, allows us to estimate the sums $S_a(M,N)$ nontrivially, provided N and t are large enough. In turn, this shows that, under the same conditions, the roots $\vartheta^{1/n}$, for $n = M+1, \ldots, M+N$ with $\gcd(n,t) = 1$, are uniformly distributed modulo p.

2000 *Mathematics Subject Classification*: Primary 11L07, 11L20, 11T23.
Key words and phrases: exponential sums, modular roots, uniform distribution.

Furthermore, this bound implies a nontrivial estimate for the sums over primes

$$T_a(L) = \sum_{\substack{l\le L\\ \gcd(l,t)=1\\ l \text{ prime}}} \mathbf{e}_p(a\vartheta^{1/l}), \qquad a \in \mathbb{F}_p.$$

Again, exponential sums with prime powers ϑ^l have recently been considered in the literature (see [1, 4, 16]).

Our bound of the sums $T_a(L)$ follows naturally by the Vaughan method from our bound of $S_a(M,N)$ and of certain bilinear sums which we estimate using some results of [4]. Similar bilinear sums have been estimated in a number of works [1, 4, 12, 14, 15], thus our estimate of these sums follows a well established path. It is interesting to note that usually bounds of bilinear sums present the main difficulty in estimating exponential sums over primes. However, in the case of the function $\vartheta^{1/l}$ the technique for establishing such bounds has been readily available, while finding a nontrivial bound on single sums $S_a(M,N)$ has been the missing element.

Finally, we discuss some applications of our results to pseudorandom number generators.

Throughout the paper the implied constants in symbols "O" and "$\ll$" may occasionally, where obvious, depend on the small positive parameter ε and are absolute otherwise (we recall that $A \ll B$ is equivalent to $A = O(B)$).

2. Preparations.

Our main tool is the following estimate from [5].

LEMMA 1. *For any $\varepsilon > 0$ there exists $\kappa > 0$ such that if $\vartheta_1,\dots,\vartheta_r \in \mathbb{F}_p^*$ and their ratios ϑ_i/ϑ_j, $1 \le i < j \le r$, are of multiplicative order at least p^ε then*

$$\max_{a_i\in\mathbb{F}_p^*}\Big|\sum_{s=1}^{p-1}\mathbf{e}_p\Big(\sum_{i=1}^{r} a_i\vartheta_i^s\Big)\Big| \ll p^{1-\kappa}.$$

As we have mentioned, we also need a bound of some bilinear sums.

LEMMA 2. *For any $\varepsilon > 0$ there exists $\eta > 0$ such that for $t \ge p^\varepsilon$, uniformly over $a \in \mathbb{F}_p^*$ the following holds. For any two sequences of complex numbers $\mathcal{A} = (\alpha_r)$ supported on the interval $[K, K+R]$ and $\mathcal{B} = (\beta_s)$ supported on the interval $[L, L+S]$, and for any integer a with* $\gcd(a,p) = 1$, *we have*

$$\sum_{\substack{K<r\le K+R\\ \gcd(r,t)=1}} \sum_{\substack{L<s\le L+S\\ \gcd(s,t)=1}} \alpha_r\,\beta_s\,\mathbf{e}_p(a\vartheta^{1/(rs)}) \ll \|\mathcal{A}\|\,\|\mathcal{B}\|(R/t+1)^{1/2}(S/t+1)^{1/2}t^{1-\eta}$$

where

$$\|\mathcal{A}\| = \Big(\sum_{K<r\le K+R} |\alpha_r|^2\Big)^{1/2} \quad \textit{and} \quad \|\mathcal{B}\| = \Big(\sum_{L<s\le L+S} |\beta_s|^2\Big)^{1/2}.$$

Proof. We follow the standard argument which has been applied to similar sums with ϑ^{rs} instead of $\vartheta^{1/(rs)}$ (see [1, 4]). In fact in this case there are some simplifications due to the extra condition $\gcd(rs,t)=1$.

Let us fix an $a \in \mathbb{F}_p^*$ and denote the corresponding bilinear sums by W.

Using the Cauchy inequality, we find

$$\begin{aligned}
W^2 &\le \sum_{K<r\le K+R} |\alpha_r|^2 \sum_{K<r\le K+R} \Big| \sum_{\substack{L<s\le L+S\\ \gcd(s,t)=1}} \beta_s \, \mathbf{e}_p(a\vartheta^{1/(rs)})\Big|^2 \\
&\le \|\mathcal{A}\|^2 (R/t+1) \sum_{r\in\mathbb{Z}_t^*} \Big| \sum_{\substack{L<s\le L+S\\ \gcd(s,t)=1}} \beta_s \, \mathbf{e}_p(a\vartheta^{1/(rs)})\Big|^2 \\
&\le \|\mathcal{A}\|^2 (R/t+1) \sum_{r\in\mathbb{Z}_t} \Big| \sum_{\substack{L<s\le L+S\\ \gcd(s,t)=1}} \beta_s \, \mathbf{e}_p(a\vartheta^{r/s})\Big|^2 \\
&= \|\mathcal{A}\|^2 (R/t+1) \sum_{\substack{L<s,v\le L+S\\ \gcd(s,t)=\gcd(v,t)=1}} \beta_s \, \overline{\beta}_v \sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^{r/s}-\vartheta^{r/v})).
\end{aligned}$$

Since

$$2|\beta_s\overline{\beta}_v| \le |\beta_s|^2 + |\beta_v|^2,$$

we deduce that

$$\begin{aligned}
W^2 &\le \frac{1}{2}\|\mathcal{A}\|^2 (R/t+1) \sum_{\substack{L<s,v\le L+S\\ \gcd(s,t)=\gcd(v,t)=1}} |\beta_s|^2 \Big| \sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^{r/s}-\vartheta^{r/v}))\Big| \\
&\quad + \frac{1}{2}\|\mathcal{A}\|^2 (R/t+1) \sum_{\substack{L<s,v\le L+S\\ \gcd(s,t)=\gcd(v,t)=1}} |\beta_v|^2 \Big| \sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^{r/s}-\vartheta^{r/v}))\Big| \\
&= \|\mathcal{A}\|^2 (R/t+1) \sum_{\substack{L<s,v\le L+S\\ \gcd(s,t)=\gcd(v,t)=1}} |\beta_s|^2 \Big| \sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^{r/s}-\vartheta^{r/v}))\Big| \\
&\le \|\mathcal{A}\|^2 (R/t+1)(S/t+1) \sum_{\substack{L\le s\le L+S\\ \gcd(s,t)=1}} |\beta_s|^2 \sum_{v\in\mathbb{Z}_t^*} \Big| \sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^{r/s}-\vartheta^{r/v}))\Big|.
\end{aligned}$$

For each s, we make the change of variables $r \mapsto rs$, $v \mapsto v^{-1}s$. Therefore,

$$W^2 \le \|\mathcal{A}\|^2(R/t+1)(S/t+1) \sum_{\substack{L\le s\le L+S\\ \gcd(s,t)=1}} |\beta_s|^2 \sum_{v\in\mathbb{Z}_t^*}\Big|\sum_{r\in\mathbb{Z}_t} \mathbf{e}_p(a(\vartheta^r-\vartheta^{rv}))\Big|.$$

The double sum over v and r does not depend on s and is $O(t^{2-2\kappa})$ by [4, Theorem 4] for some $\kappa > 0$ (provided that $t \ge p^{\varepsilon}$), which concludes the proof. ■

Let, as usual,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of a prime } p,\\ 0 & \text{otherwise,}\end{cases}$$

be the von Mangoldt function, where $\log z$ denotes the natural logarithm of z.

We use the following result of [29] in the form given in [11, Chapter 24]:

Lemma 3. *For any complex-valued function $f(n)$ and any real numbers $U, V > 1$ with $UV \le L$, we have*

$$\sum_{n\le L} \Lambda(n) f(n) \ll \Sigma_1 + \Sigma_2 + \Sigma_3 + |\Sigma_4|,$$

where

$$\Sigma_1 = \Big|\sum_{n\le U} \Lambda(n)f(n)\Big|,$$

$$\Sigma_2 = (\log UV) \sum_{v\le UV}\Big|\sum_{s\le L/v} f(sv)\Big|,$$

$$\Sigma_3 = (\log L) \sum_{v\le V} \max_{w\ge 1}\Big|\sum_{w\le s\le L/v} f(sv)\Big|,$$

$$\Sigma_4 = \sum_{\substack{km\le L\\ k>V,\, m>U}} \Lambda(m)\Big|\sum_{d\mid k,\, d\le V} \mu(d)\Big| f(km).$$

3. Sums over consecutive integers. Following the usual approach to estimating incomplete sums (see [18, Section 12.2]), we first estimate the complete sums

$$S_{a,b} = \sum_{n\in\mathbb{Z}_t^*} \mathbf{e}_p(a\vartheta^{1/n})\mathbf{e}_t(bn).$$

Theorem 4. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for $t \ge p^{\varepsilon}$, uniformly over $a \in \mathbb{F}_p^*$ and $b \in \mathbb{Z}_t$, we have the bound*

$$S_{a,b} \ll t^{1-\delta}.$$

Proof. For any integer $k \ge 2$,

$$S_{a,b}^k = \sum_{n_1,\dots,n_k \in \mathbb{Z}_t^*} \mathbf{e}_p\Big(a\sum_{j=1}^k \vartheta^{1/n_j}\Big)\mathbf{e}_t\Big(b\sum_{j=1}^k n_j\Big).$$

For each $m \in \mathbb{Z}_t$, we collect together the terms with $n_1 + \cdots + n_k \equiv m \pmod t$, getting

$$|S_{a,b}|^k \le \sum_{m\in\mathbb{Z}_t}\Big|\sum_{\substack{n_1,\dots,n_k\in\mathbb{Z}_t^*\\ n_1+\cdots+n_k\equiv m \,(\mathrm{mod}\, t)}} \mathbf{e}_p(a(\vartheta^{1/n_1}+\cdots+\vartheta^{1/n_k}))\Big|.$$

Next, by the Cauchy inequality, we derive

$$\begin{aligned}|S_{a,b}|^{2k} &\le t\sum_{m\in\mathbb{Z}_t}\Big|\sum_{\substack{n_1,\dots,n_k\in\mathbb{Z}_t^*\\ n_1+\cdots+n_k\equiv m \,(\mathrm{mod}\, t)}} \mathbf{e}_p\Big(a\sum_{j=1}^k \vartheta^{1/n_j}\Big)\Big|^2\\ &= t\sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k}\mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j\vartheta^{1/n_j}\Big),\end{aligned}$$

where the outside summation is taken over the set of vectors

$$\begin{aligned}\mathcal{N}_k = \{&(n_1,\dots,n_{2k})\in(\mathbb{Z}_t^*)^{2k} :\\ &n_1+n_3+\cdots+n_{2k-1}\equiv n_2+n_4+\cdots+n_{2k} \pmod t\}.\end{aligned}$$

It is now easy to see that for any m with $\gcd(m,t)=1$ we have

$$\sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k}\mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j\vartheta^{1/n_j}\Big) = \sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k}\mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j\vartheta^{m/n_j}\Big).$$

Let $\mathcal{Q}$ be the set of primes $q \le t^{3/4}$ with $\gcd(q,t)=1$. Averaging over all $q\in\mathcal{Q}$ we obtain

$$|S_{a,b}|^{2k} \le \frac{t}{\#\mathcal{Q}}\sum_{q\in\mathcal{Q}}\sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k}\mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j\vartheta^{q/n_j}\Big).$$

Furthermore, changing the order of summation, we obtain

$$|S_{a,b}|^{2k} \le \frac{t}{\#\mathcal{Q}}\sum_{(n_1,\dots,n_{2k})\in\mathcal{N}_k}\Big|\sum_{q\in\mathcal{Q}}\mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j\vartheta^{q/n_j}\Big)\Big|.$$

Clearly $\#\mathcal{N}_k \le \varphi(t)^{2k-1}$, where $\varphi(t)$ is the Euler function. Since t has at most $O(\log t)$ prime divisors, by the prime number theorem we see that $\#\mathcal{Q} \ge (4/3+o(1))t^{3/4}/\log t + O(\log t) \ge t^{3/4}/\log t$, provided t is large enough.

Now, using the Hölder inequality and then extending the region of summation, we derive

$$\begin{aligned}
|S_{a,b}|^{8k} &\le \frac{t^4}{(\#\mathcal{Q})^4}(\#\mathcal{N}_k)^3 \sum_{(n_1,\ldots,n_{2k})\in\mathcal{N}_k} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j \vartheta^{q/n_j}\Big)\Big|^4\\
&\le t^{6k-2}(\log t)^4 \sum_{\substack{n_1,\ldots,n_{2k}=1\\ \gcd(n_1\cdots n_{2k},t)=1}}^{t} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j \vartheta^{q/n_j}\Big)\Big|^4\\
&\le t^{6k-2}(\log t)^4 \sum_{n_1,\ldots,n_{2k}=1}^{t} \Big|\sum_{q\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(-1)^j \vartheta^{q n_j}\Big)\Big|^4\\
&\le t^{6k-2}(\log t)^4\\
&\qquad\times \sum_{n_1,\ldots,n_{2k}=1}^{t} \sum_{q_1,q_2,q_3,q_4\in\mathcal{Q}} \mathbf{e}_p\Big(a\sum_{j=1}^{2k}(\vartheta^{q_1 n_j}+\vartheta^{q_2 n_j}-\vartheta^{q_3 n_j}-\vartheta^{q_4 n_j})\Big)\\
&\le t^{6k-2}(\log t)^4\\
&\qquad\times \sum_{q_1,q_2,q_3,q_4\in\mathcal{Q}} \Big|\sum_{n=1}^{t} \mathbf{e}_p(a(\vartheta^{q_1 n}+\vartheta^{q_2 n}-\vartheta^{q_3 n}-\vartheta^{q_4 n}))\Big|^{2k}\\
&\le \Big(\frac{t}{p-1}\Big)^{2k} t^{6k-2}(\log t)^4\\
&\qquad\times \sum_{q_1,q_2,q_3,q_4\in\mathcal{Q}} \Big|\sum_{n=1}^{p-1} \mathbf{e}_p(a(\vartheta^{q_1 n}+\vartheta^{q_2 n}-\vartheta^{q_3 n}-\vartheta^{q_4 n}))\Big|^{2k}\\
&\ll p^{-2k}t^{8k-2}(\log t)^4\\
&\qquad\times \sum_{q_1,q_2,q_3,q_4\in\mathcal{Q}} \Big|\sum_{n=1}^{p-1} \mathbf{e}_p(a(\vartheta^{q_1 n}+\vartheta^{q_2 n}-\vartheta^{q_3 n}-\vartheta^{q_4 n}))\Big|^{2k}.
\end{aligned}$$

For $O((\#\mathcal{Q})^2) = O(t^{3/2})$ tuples $(q_1,q_2,q_3,q_4)\in\mathcal{Q}^4$ such that (q_1,q_2) is a permutation of (q_3,q_4) we estimate the inner sum trivially as $p-1$.

For other $O((\#\mathcal{Q})^4) = O(t^3)$ tuples, noticing that if $q_i \ne q_j$ then

$$\gcd(q_i-q_j,t) \le |q_i-q_j| \le t^{3/4}, \qquad 1\le i<j\le 4,$$

we see that the bound of Lemma 1 applies. Therefore

$$\begin{aligned}
|S_{a,b}|^{8k} &\ll p^{-2k}t^{8k-2}(t^3p^{2k(1-\kappa)}+t^{3/2}p^{2k})(\log t)^4\\
&\ll (t^{8k+1}p^{-2k\kappa}+t^{8k-1/2})(\log t)^4,
\end{aligned}$$

with some $\kappa>0$, depending only on $\varepsilon>0$. Taking $k=\lceil\kappa^{-1}\rceil$ we conclude the proof. ∎

The standard technique (see [18, Section 12.2]) now immediately leads us to the following estimate of the sums $S_a(M,N)$.

Corollary 5. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for $t \ge p^{\varepsilon}$, uniformly over $a \in \mathbb{F}_p^*$ and integers M and N with $1 \le N \le t$, we have*

$$S_a(M,N) \ll t^{1-\gamma}.$$

4. Sums over primes

Theorem 6. *For any $\varepsilon > 0$ there exists $\sigma > 0$ such that for $t \ge p^{\varepsilon}$, uniformly over $a \in \mathbb{F}_p^*$ and integer $L \ge t^{2+\varepsilon}$, we have the bound*

$$T_a(L) \ll Lt^{-\sigma}.$$

Proof. Our proof follows very closely to the proof of [4, Theorem 6] which gives an estimate of exponential sums with ϑ^l. In particular, we also choose $U = V = t$ in the Vaughan identity given by Lemma 3. Then, exactly as in [4, Theorem 6],

- we estimate Σ_1 trivially as $\Sigma_1 \le t$,
- we estimate $\Sigma_2 \ll Lt^{-\varrho}$ and $\Sigma_3 \ll Lt^{-\varrho}$ using Corollary 5 instead of [4, Theorem 4],
- we estimate $\Sigma_4 \ll Lt^{-\varrho}$ using Lemma 2 instead of [4, Bounds (57) and (58)] on the double sum in [4, Bound (55)],

where $\varrho > 0$ depends only on ε. Collecting these bounds together, we obtain

$$\sum_{\substack{n \le L\\ \gcd(n,t)=1}} \mathbf{e}_p(a\vartheta^{1/n}) \ll Lt^{-\varrho},$$

and now via partial summation we obtain the desired result. ■

5. Remarks. Clearly, consecutive iterations of the map $x \mapsto \vartheta x$ in $\mathbb{F}_p$ lead to the sequence $x_n = a\vartheta^n$, $n = 0,1,\ldots,$ where $x_0 = a$ is the initial value. For many years such sequences have served as sources of pseudorandom numbers (see [20, 27, 28]). However, unfortunately such sequences are not suitable for cryptographic applications, because even some of the information about the output sequence is discarded (for example, only some portion of the most significant bits of each x_n is output), the attacker is still able to find the "hidden" parameters a and ϑ (and in some cases even if p is unknown, it can also be recovered); see [8, 9, 10, 13, 19, 24, 25]. Moreover, even iterations of nonlinear maps can be attacked in a similar way (see [2, 3]).

Thus, in this context, it seems quite promising to use the sequence $z_n = a\vartheta^{1/n}$ for the purpose of creating cryptographically strong pseudorandom number generators (one can choose $\vartheta \in \mathbb{F}_p$ to be of prime order t to avoid problems with inverting n modulo t). In particular, the bound of Corollary 5 implies that elements of such sequences are uniformly distributed in residue classes modulo p. In this context it would also be interesting to extend our method to the sums

$$\sum_{\substack{n=M+1\\ \gcd((n+1)\cdots(n+s),t)=1}}^{M+N} \mathbf{e}_p\Big(\sum_{j=1}^{s} a_j \vartheta^{1/(n+i)}\Big),$$

which are necessary to study the joint distribution of s consecutive terms of the sequence z_n.

Finally, we remark that our argument can easily be adapted to apply to the sums

$$\sum_{\substack{n=M+1\\ \gcd(n,t)=1}}^{M+N} \mathbf{e}_p\Big(\sum_{j=1}^{s} a_j \vartheta_j^{1/n}\Big),$$

for distinct elements $\vartheta_1, \ldots, \vartheta_s$ of order t.

Acknowledgments. The authors are grateful to the anonymous referee for a careful reading of the manuscript and valuable remarks.

References

[1] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, *Exponential sums with Mersenne numbers*, Compos. Math. 140 (2004), 15–30.

[2] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, *Predicting the inversive generator*, in: Cryptography and Coding, Lecture Notes in Comput. Sci. 2898, Springer, Berlin, 2003, 264–275.

[3] —, —, —, —, *Predicting nonlinear pseudorandom number generators*, Math. Comp. 74 (2005), 1471–1494.

[4] J. Bourgain, *Estimates on exponential sums related to Diffie–Hellman distributions*, Geom. Funct. Anal. 15 (2005), 1–34.

[5] —, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18 (2005), 477–499.

[6] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. 73 (2006), 380–398.

[7] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris 337 (2003), 75–80.

[8] J. Boyar, *Inferring sequences produced by pseudo-random number generators*, J. ACM 36 (1989), 129–141.

[9] —, *Inferring sequences produced by a linear congruential generator missing low-order bits*, J. Cryptology 1 (1989), 177–184.

[10] S. Contini and I. E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, in: Information Security and Privacy (Brisbane, 2005), Lecture Notes in Comput. Sci. 3574, Springer, Berlin, 2005, 52–60.

[11] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, New York, 1980.

[12] J. B. Friedlander and I. E. Shparlinski, *Double exponential sums over thin sets*, Proc. Amer. Math. Soc. 129 (2001), 1617–1621.

[13] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias and A. Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM J. Comput. 17 (1988), 262–280.

[14] M. Z. Garaev, *Double exponential sums related to Diffie–Hellman distributions*, Int. Math. Res. Notices 2005, no. 17, 1005–1014.

[15] M. Z. Garaev and A. A. Karatsuba, *New estimates of double trigonometric sums with exponential functions*, J. Number Theory 114 (2005), 182–192.

[16] M. Z. Garaev and I. E. Shparlinski, *The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes*, Int. Math. Res. Notices 2005, no. 39, 2391–2408.

[17] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221–235.

[18] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[19] A. Joux and J. Stern, *Lattice reduction: A toolbox for the cryptanalyst*, J. Cryptology 11 (1998), 161–185.

[20] D. Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading, MA, 1998.

[21] S. V. Konyagin and I. Shparlinski, *Character Sums with Exponential Functions and their Applications*, Cambridge Univ. Press, Cambridge, 1999.

[22] N. M. Korobov, *On the distribution of digits in periodic fractions*, Math. USSR-Sb. 18 (1972), 659–676.

[23] —, *Exponential Sums and their Applications*, Kluwer, Dordrecht, 1992.

[24] H. Krawczyk, *How to predict congruential generators*, J. Algorithms 13 (1992), 527–545.

[25] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, in: Proc. Sympos. Appl. Math. 42, Amer. Math. Soc., Providence, RI, 1990, 115–143.

[26] H. L. Montgomery, *Distribution of small powers of a primitive root*, in: Advances in Number Theory, Clarendon Press, Oxford, 1993, 137–149.

[27] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. 84 (1978), 957–1041.

[28] —, *Random Number Generation and Quasi–Monte Carlo Methods*, SIAM Press, Philadelphia, 1992.

[29] R. C. Vaughan, *An elementary method in prime number theory*, Acta Arith. 37 (1980), 111–115.

Institute for Advanced Study
Princeton, NJ 08540, U.S.A.
E-mail: bourgain@ias.edu

Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor@ics.mq.edu.au

Received on 25.9.2007
and in revised form on 25.1.2008 (5540)